

IN THE SPECIFICATION

Please amend the paragraph at page 4, line 26 through page 5, line 7 as follows:

To overcome this problem, there is proposed an expanded key scheduling section shown in FIG. 39 ~~49~~. The generating section comprises the round processors 1001_1 to 1001_n connected in series, round processors 1021_n to 1021_2 connected in series, the round processor 1021_n being connected to the round processor 1001_n , the expanded key converters 1005_1 to 1005_n respectively connected to outputs of the expanded key processors 1021_2 to 1021_n , and 1001_n .